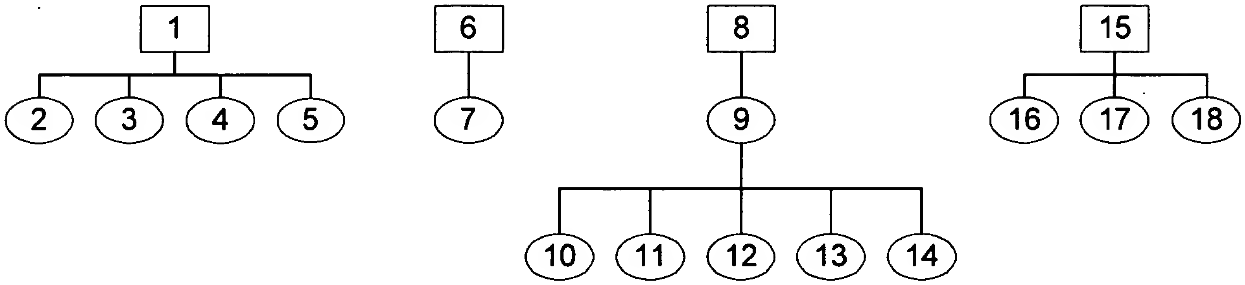
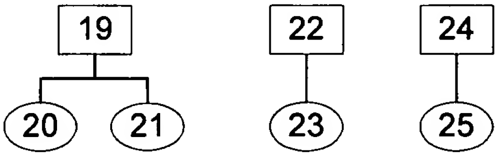
REMARKS

Claims 1-18 are pending in this application. Currently no claims stand allowed. The diagram below illustrates the relationships among the various pending claims. Claims 1, 6, 8, and 15 are in independent form.



The Office Action rejects claims 1-18 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent 6,389,462 to Cohen et al. (*Cohen*) in view of U.S. Patent 6,243,815 to Antur et al. (*Antur*). Independent claims 1, 6, 8, and 15 have additionally been rejected under 35 U.S.C. § 103(a) as being unpatentable over what the Office Action regards as "Applicants' Admitted Prior Art" in view of *Antur*.

Although applicants do not agree that pending claims 1-18 are obvious over the prior art of record, applicants have nevertheless elected to cancel these claims in favor of new claims 19-25, in which claims 19, 22, and 24 are in independent form as illustrated in the following diagram:



Claims 19-25 are aimed at more distinctly pointing out that applicants' invention relates to a proxy firewall device performing network address translation (NAT) and application-level filtering functions. In the prior art, these functions are handled by separate elements of an internal computer network. Claims 19-25 further emphasize that the filtering of packets is accomplished in a manner that is transparent to the client in the internal network. The references discussed in the Office Action do not teach or suggest a reason for combining these distinctive features.

Specifically, in contrast to *Cohen*, which is concerned with proxy caching to reduce web object retrieval latency, claims 19-25 (like the previous claims) concern the use of a proxy server as a firewall, which improves security in data communications across an external network. For example, independent claim 19 recites "[*a*] *method for securing data communication between a client in an internal network and a server in an external network by way of a proxy server*". Similarly, independent claim 22 recites "[*a*] *system for securing data communication across an external computer network*" in which the security is provided by a "*proxy device*" containing components for performing NAT and application-level filtering.

Moreover, *Cohen* teaches a proxy redirector switching entity that is separate from, and transparent to, proxy caches in the internal network. *Cohen*, col. 4, ll. 44-49. The separate proxy redirector, not the proxy cache, performs NAT, for example. Id. at col. 15, ll. 9-34. In suggesting that network proxy functions should be divided among separate network entities, *Cohen* **teaches away** from claims 19-25, which describe a combination of NAT and application-level gateway functions in one network firewall device.

In independent claim 19, the recited steps are all performed "*at the proxy server*," as are the reverse-direction steps in dependent claim 20. In independent claim 22 and dependent claim 23, "*a proxy device in the internal computer network*" contains the components that provide both NAT and filtering. Independent claim 24 and dependent claim 25 are directed to "[*a*] *proxy device located in an internal network*"; this single proxy device comprises routines for performing NAT and transparent filtering.

The Office Action implies that Figures 1 and 3 of *Cohen* teach a NAT/proxy device (see Office Action ¶ 12, discussing independent claim 8). However, these drawing figures do not teach a single network device performing both NAT and proxy functions, as set forth in claims 19-25. The proxy redirector 104 and the proxy cache 115 are shown as separate network devices, and the proxy redirector performing the method illustrated in Figure 3 is distinct from the set of proxy caches in the network (see *Cohen* at Fig. 3, steps 302 and 305-306).

The Office Action contends that it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the method of packet filtering described in *Antur* with the teachings of *Cohen*, and with what it characterizes as applicants' admitted prior art, because "[*Antur*'s] method of packet filtering provides an increased form of firewall security"

(Office Action ¶¶ 7, 18). The part of the detailed description in *Antur* referenced in the Office Action simply contains a background discussion of packet filtering techniques, however, concluding that "[p]acket filtering is typically the least secure form of firewall" (*Antur* at col. 4, ll. 45-46). As with *Cohen*, *Antur* does not teach or suggest the combination of NAT and application-level gateway functions in one network firewall device, an element of applicants' invention emphasized in claims 19-25.

CONCLUSION

The application, including the amendment requested herein, is considered to be in good and proper form for allowance, and the examiner is respectfully requested to pass this application to issue.

If, in the opinion of the examiner, a telephone conference would expedite the prosecution of the subject application, the examiner is invited to call the undersigned attorney.

Respectfully submitted,

Richard E. Fontana

Richard E. Fontana, Reg. No. 52,902
One of the Attorneys for Applicants
LEYDIG, VOIT & MAYER, LTD.
Two Prudential Plaza, Suite 4900
180 North Stetson Avenue
Chicago, Illinois 60601-6780
(312) 616-5600 (telephone)
(312) 616-5700 (facsimile)

Date: August 19, 2003